A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Data Objects

Sander Oudkerk (NATO C3 Agency)

sander.oudkerk@nc3a.nato.int

Ian Bryant (UK Ministry of Defence)

ibryant@relay.mod.uk

Anders Eggen, Raymond Haakseth (Norwegian Defence Research Establishment – FFI)

{anders.eggen, raymond.haakseth}@ffi.no

ABSTRACT

This paper explores the work done by the NATO Research Task Group on XML in Cross Domain Security Solutions (IST-068/RTG-031) in developing a proposal for an XML-Labelling and metadata binding specification that aligns with the requirements for information exchange of both NATO organisations / missions and member nations. Existing solutions were found to have deficiencies in either their data structures or semantics that could impede bi-directional automated flows using access control decision functions. The XML-Labelling and binding solutions are described in two specifications proposed by IST-068/RTG-031: "XML Confidentiality Label Syntax" and "Binding of Metadata to Data Objects". This paper will provide an overview of the contents of both specifications and its application.

1.0 INTRODUCTION

1.1 NATO Research Task Group on XML in Cross Domain Security Solutions

This paper explores the work done by the NATO Research Task Group on XML in Cross Domain Security Solutions (IST-068/RTG-031). The group's goal was to improve the possibility to share information in military environments and to facilitate the evolution of a flexible infrastructure by utilizing the eXtensible Markup Language (XML) to create suitable security solutions. The group's lifetime ended in 2009 and the final report [1] will become available in 2010.

The group's major result is the work done on the development of a proposal for an XML-Labelling and Metadata Binding specification that aligns with the requirements for information exchange of both NATO organisations / missions and member nations. The XML-labelling and binding solutions are described in two specifications that are contained in the group's final report: "XML Confidentiality Label Syntax" and "Binding of Metadata to Data Objects". This paper will provide an overview of the contents of both specifications as well as the rationale behind their development.

1.2 Object Level Protection in Support of NATO Network Enabled Capabilities

The development of the XML-labelling and binding specification was done in support of the concept of Object Level Protection (OLP). OLP is one of the pillars of Information Assurance (IA) for NATO Network Enabled Capabilities (NNEC) and aims to solve the several challenges for the protection of information and resources that are specific to NNEC. The information and communication services that have to support NNEC are flexible and more specifically, the location of information and resources and the transmission paths can not always be predicted at design time of the infrastructure, or are known to be

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **NOV 2010**	2. REPORT TYPE **N/A**	3. DATES COVERED **-**

4. TITLE AND SUBTITLE **A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Data Objects**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **NATO C3 Agency**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

See also ADA564697. Information Assurance and Cyber Defence (Assurance de l'information et cyberdefense). RTO-MP-IST-091

14. ABSTRACT

This paper explores the work done by the NATO Research Task Group on XML in Cross Domain Security Solutions (IST-068/RTG-031) in developing a proposal for an XML-Labelling and metadata binding specification that aligns with the requirements for information exchange of both NATO organisations / missions and member nations. Existing solutions were found to have deficiencies in either their data structures or semantics that could impede bi-directional automated flows using access control decision functions. The XML-Labelling and binding solutions are described in two specifications proposed by IST-068/RTG-031: XML Confidentiality Label Syntax and Binding of Metadata to Data Objects. This paper will provide an overview of the contents of both specifications and its application.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**10**	

variable. To maintain flexibility the protection of information and resources has to be adaptable to operational requirements that may vary by location or over time. Further, information needs to be shared between coalitions partners while at the same time respecting security policies and certain cases of information sharing between different security domains need to be automated.

Whereas these challenge are difficult to solve using the classical approaches to protection of information and resources, OLP has two aspects which make it different from classical approaches:

- Protection mechanisms can be provided at a fine level of granularity; more specifically, instead of providing the same protection to, for instance, all information and resources within an entire network enclave, protection is applied to individual data objects.
- Using IA metadata, data objects can inform and control the infrastructure and its protection mechanisms about security requirements for the protection of the data objects.

The concepts of a data object and metadata are central to OLP. The general idea is that protection mechanisms may use IA metadata associated with a data object in order to provide their services for the data object. For this the metadata may be provided in combination with the data object or may be provided separately. For instance, the metadata may be part of the data object or may be retrieved from a central repository.As the metadata can be detached from the data object, the association between the data object and its IA metadata needs to be represented in some form. In the concept of OLP this is achieved by a so-called *Binding*. The binding relates data object and IA metadata. The combination of IA metadata and binding data is called a *Security Label* in the terms of the traditional markup[1] for human readable documents (often the binding is implicit by inclusion of label in the data object).

1.3 XML

The development of the labelling and binding specifications centered upon the use of XML; it is generally considered as the “lingua franca” for most future information exchange and interoperability requirements, and is a component of military communications and information systems currently on the agenda of many NATO nations and NATO organisations in the context of Service Oriented Architectures. The emergent use of XML in many data object structures suggests that XML based labels are most appropriate for future capabilities to support operations. In addition, the structure of XML is inherently suitable to allow for the provision of access control with a fine level of granularity.

2.0 GENERAL DESIGN CONSIDERATIONS

2.1 Approach

The XML-Labelling and binding specification were designed to support the concept of OLP by developing a generic method to bind any type of metadata to any type of data object while allowing access control decision functions (ACDF) to enforce an access control policy at a fine level of granularity. In addition, the use of a standardized binding and format of an XML-based security label will help to establish clear semantics of the label, allowing ACDF to be application or data format agnostic which will simplify the development of common trusted ACDF in an NNEC environment such as cross-domain release mechanisms, e.g. guards. A non-standardized approach would force such ACDF to support a plethora of data and label formats. This will typically increase the complexity of ACDF implementation and management of access control policies, hampering the enforcement of security policies with a higher level of assurance.

[1] Expressing Policy Identifier, Classification and Release categories (caveats).

Establishing a generic way of data labelling and binding in support of OLP naturally involves making design considerations and trade-offs. The remainder of this section summarises the inherent limiting conditions that provided the fundamental requirements for the design of the specifications.

2.2 Naming Convention

Traditionally the term ‘security label’ is used for constructs describing the sensitivity of content (where the term label is used for the ‘set of metadata’ representing the sensitivity). However, as the sensitivity information in a label conveys confidentiality constraints[2], a more suitable name is ‘confidentiality label’. This is also in line with the expectation that future types of security labels may also convey constraints with respect to integrity and availability of data objects. The term ‘security label’, or ‘information assurance’ label, would then be used for the overarching label that contains confidentiality, integrity and availability labels. Such a ‘security label’ can easily be extended by including other IA related metadata.

2.3 Data Format Agnostic

As it must be possible to apply the label to all types of finite[3] data, no assumptions can be made on how the label is to be bound to the data object and therefore the labelling and binding specifications cannot mandate any requirements on the data (object) format. Also, the assumption is that existing data formats cannot be changed to accommodate the specification. In general, maintaining a separation between label and data formats enables an independent evolution of both so that a change in one will not affect the other.

2.4 Binding Mechanism

Traditionally the binding of label and data is realized by inclusion of the label in the data (object), e.g. as header or footer in a document or first line of text in e-mail messages. A strong binding is then realized by digitally signing the data object (with included label). Since in a general approach to OLP no assumptions can be made about the format of the data, the method of binding by embedding the label is not a valid general approach. Hence the label must be designed as a separate data element and a general binding mechanism is needed that can describe the relationship between the data object and the label (and any other future type of metadata that is to be bound to the data object). As a result, the binding cannot be included in the label and the binding is thus separated and represented in a data element of its own.

2.5 Reuse of Existing Standards

One of the major design tenets through the process was to reuse existing standards as far as possible. Although existing standards were not found to adequately meet government and defence security requirements, means were developed by which these standards can be augmented or adapted to achieve interoperability for NNEC. In general, reusing existing and agreed standards provides the basis for interoperability between products. Also, using standards allows for use of Commercial of the Shelve (COTS) software. Using COTS should make a faster development process with lower costs possible.

[2] In other words: based on the sensitivity information, access control decision functions typically enforce a policy with respect to confidentiality protection.

[3] How to apply a label to streams of data was out of scope for IST-068/RTG-031.

3.0 XML CONFIDENTIALITY LABEL SYNTAX

3.1 Machine Readable and Eye Readable Representations

A confidentiality label may be bound to data objects in order to express the sensitivity of the content. The sensitivity information in a confidentiality label can be compared with a user's authorizations to determine if the user is allowed to access the content. Confidentiality labels may also be used for other purposes such as a source of routing information or release control for information traversing different security domains.

In case a confidentiality label is processed by software or a system, as opposed to humans, the label syntax must meet the requirements for machine readable labels. As a minimum this requires the electronic markings to be precise and as tightly specified as possible. The design of the confidentiality label allows for both eye readable and machine readable representations of the confidentiality label. Examples are provided in Section 5.2.

3.2 Design of the XML Confidentiality Label

The generic design of the confidentiality label is shown in Figure 1 below. It consists of a parent element called ConfidentialityLabel with the mandatory element ConfidentialityInformation and the optional elements OriginatorID, CreationDateTime and SuccessionHandling. In addition, the ConfidentialityLabel element has two optional attributes: the Id attribute can be used to provide a unique identifier (the uniqueness of the identifier is only guaranteed within an instance of an XML document) and the second attribute ReviewDateTime can be used to refer to the date after which the label shall be manually reviewed.

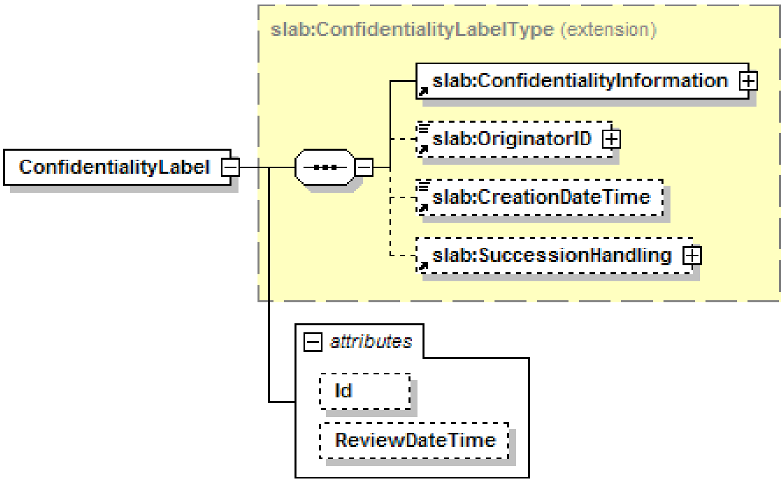


Figure 1: Design of the ConfidentialityLabel element; the ReviewDateTime attribute and the SuccessionHandling element allow for management of the time period for which the sensitivity markings captured in the ConfidentialiyInformation element remain valid

The mandatory ConfidentialityInformation element contains the traditional policy identifier, classification and category information. Of these, the policy identifier and classification are mandatory and can only appear once. The category element is optional and can be used multiple times.

The optional elements OriginatorID and CreationDateTime provide additional information on the creation of the label. The OriginatorID can be used to identify the creator of the ConfidentialityLabel. The identity itself must be represented as a string, and a type attribute can be used to define what type of ID is used. This should be flexible enough to cater for different types of identity schemes. The CreationDateTime element can be used to express the date and time of the original classification or label creation.

3.3 Automated Downgrading of the Sensitivity Level

The final optional child element of the ConfidentialityLabel element in Figure 1 above is the SuccessionHandling element. This element allows the label creator to define a confidentiality label that will succeed the current label after a given date and time. This meets the current operational requirement to capture an expected downgrade of the sensitivity level of a data object in a label. The element consists of two child elements, one specifying the date and time when the current label shall be succeded and one element containing the actual successor label. The successor label is in fact of type ConfidentialityLabel (and hence a nested, or 'recursive', label). As a result the successor label might itself ontain another successor label.

4.0 BINDING OF METADATA TO DATA OBJECTS

4.1 Loose vs. Strong Binding

The confidentiality label is essentially metadata describing the sensitivity of a given data object (information). A metadata binding provides additional information specifying which metadata belongs to which data asset and provides a verifiable reference between metadata and data. Requirements for the level of trust that a binding must offer will differ per environment. A loose binding provides a reference between the metadata and the data. This reference can be structurally verified to be correct. However, no assumptions besides this can be made. In contrast, strong bindings typically involve the use of cryptography, and cryptographic signatures are used to provide a certain level of integrity protection.

The proposed specification "Binding of Metadata to Data Objects" defines a loose binding of metadata and data object, but does not mandate a specific method for strong bindings. However, the use of the XML signature standard (XMLDSIG, [2]) is recommended and captured in a NATO profile for the binding of metadata to data objects (see Section 5.3). Both loose and strong binding can be used to bind any type of metadata to any type of data. There is no requirement that either metadata or data, or both must be defined in XML. This provides a large degree of flexibility that is desirable since all data and metadata that are in common use presently can be covered and there is no dependency on future data or metadata formats.

4.2 Granularity of Access Control

The binding mechanism allows for binding of metadata to portions of an XML data object and as such provides great flexibility and granularity in access control, e.g. a guard can redact parts of a document based on the binding information. By digitally signing the metadata, data and the binding, protection of the integrity and authenticity of all three components is realized.

Figure 2 below shows the general design of the metadata binding mechanism. The parent element MetadataBindingContainer can have one or multiple child elements named MetadataBinding. Each MetadataBinding element defines the loose binding between its child elements: Metadata (or a reference to external metadata), and Data (or a reference to external data).

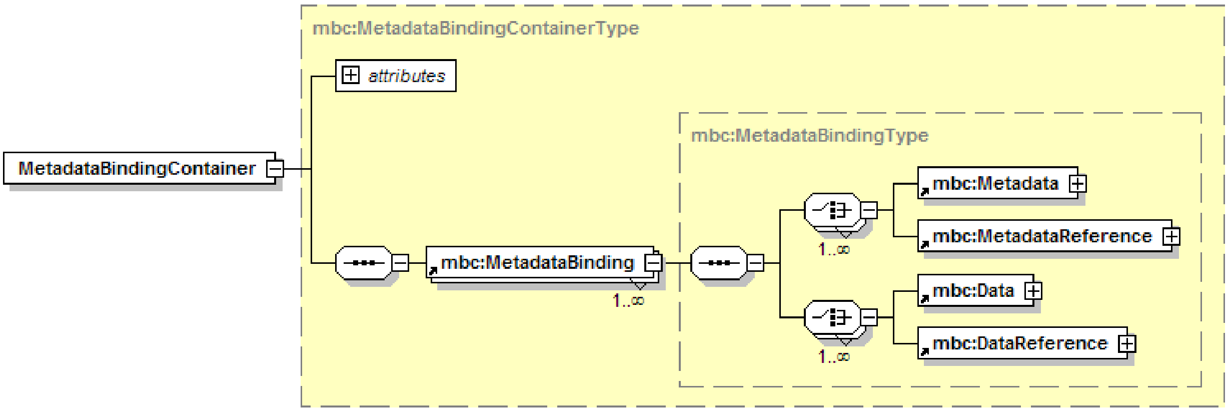


Figure 2: Design of the MetadataBindingContainer element; data (or external data by reference) and metadata (or external metadata by reference) are loosely bound by having the same parent element MetadataBinding. A strong binding can be realized by signing the MetadataBindingContainer using e.g. XMLDSIG

The MetadataBinding element can in fact be used to bind metadata to several data elements, which is useful in scenarios were the same metadata applies to several data elements or documents. For instance, a confidentiality label can apply to several parts of a document or message. The net effect of this is that less processing, storage and transmission resourses are needed. Even more, the MetadataBinding element can also be used to bind more than one metadata element to the data; this is useful when several metadata elements apply to the same data.

The mechanisms that are used to establish the binding clearly define which data objects (or parts thereof[4]) are associated with given metadata, thereby ensuring there is no ambiguity as to the semantics of the binding. This is a necessary condition for ACDF to correctly enforce an access control policy. Note that if the format of the data object that is labelled is XML, then label and binding can be embedded in the data object (together with the signature if XMLDSIG is used to realize the binding).

4.3 Original vs. Alternative Confidentiality Label

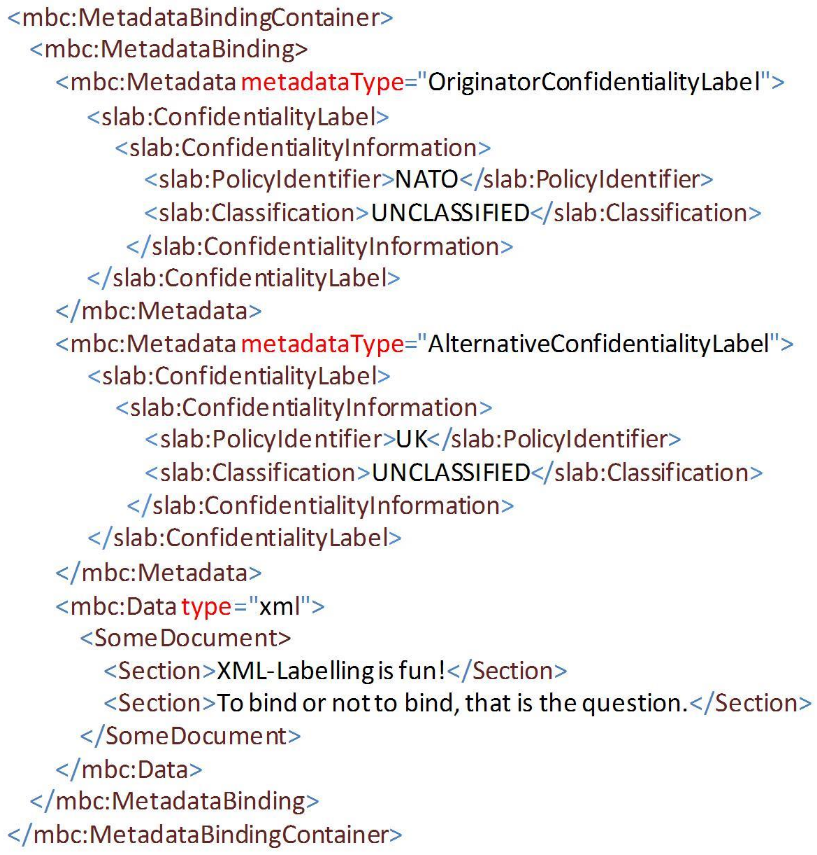
The proposed specification defines three types of metadata: ‘OriginatorConfidentialityLabel’, ‘AlternativeConfidentialityLabel’ and a generic type ‘Metadata’. The first two types involve metadata that is defined by the ConfidentialityLabel element (see Section 3.2). Note that only one metadata element of type OriginatorConfidentialityLabel can be added to the MetadataBinding. As its name suggest this type of metadata is to be used when the original confidentiality label applies, which is the default.

If an ACDF is unable to interpet the original confidentiality label it may make use of an alternative confidentiality label stored in the metadata type AlternativeConfidentialityLabel. The alternative confidentiality label is typically a (bilaterally agreed) national equivalent label[5]. The third type defined for metadata is intended for use if general metadata is bound to the data. The list of metadata types can and should be extended in the future.

[4] When the data object is XML, XPath expressions or XPointers can be used to identify a subset of the data object.

[5] For example, a NATO UNCLASSIFIED document may get the alternative label UK UNCLASSFIED upon crossing a domain boundary from the NATO domain into the UK domain. The alternative label is used by ACDF in the UK domain, however the original label is kept to trace origin. When the NATO UNCLASSIFIED document leaves the UK domain, the alternative (UK) label is removed.

Figure 3 below shows a (mock) example of a MetadataBindingContainer element containing a MetadataBinding element that (loosely) binds an original and alternative confidentiality label to (XML) data. The original confidentiality label shows that the data object originated in the NATO domain. In this example, an ACDF in the UK domain that is unable to interpret the NATO policy would interpret the alternative label[6] instead:



```
<mbc:MetadataBindingContainer>
  <mbc:MetadataBinding>
    <mbc:Metadata metadataType="OriginatorConfidentialityLabel">
      <slab:ConfidentialityLabel>
        <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
          <slab:Classification>UNCLASSIFIED</slab:Classification>
        </slab:ConfidentialityInformation>
      </slab:ConfidentialityLabel>
    </mbc:Metadata>
    <mbc:Metadata metadataType="AlternativeConfidentialityLabel">
      <slab:ConfidentialityLabel>
        <slab:ConfidentialityInformation>
          <slab:PolicyIdentifier>UK</slab:PolicyIdentifier>
          <slab:Classification>UNCLASSIFIED</slab:Classification>
        </slab:ConfidentialityInformation>
      </slab:ConfidentialityLabel>
    </mbc:Metadata>
    <mbc:Data type="xml">
      <SomeDocument>
        <Section>XML-Labelling is fun!</Section>
        <Section>To bind or not to bind, that is the question.</Section>
      </SomeDocument>
    </mbc:Data>
  </mbc:MetadataBinding>
</mbc:MetadataBindingContainer>
```

Figure 3: Example of a MetadataBindingContainer element; an original and alternative confidentiality label are (loosely) bound to an XML document that is included in the Data element. The Data element can be replaced by a DataReference element that could identify the same XML document by using the Uniform Resource Identifier (URI) attribute which can contain a reference, e.g. htttp://www.nato.int/someXMLdocument.xml

5.0 NATO PROFILES

5.1 Towards Interoperability

The labelling and binding specifications have been designed with flexibility in mind and allow NATO nations to tailor many details of the specification to their needs. However, for use within NATO it is beneficial to restrain some of the flexibility to fixed choices so that interoperability is more easily achieved. To this purpose, the NATO Consultation Command and Control Agency (NC3A) is in the process of developing NATO profiles for both the “XML Confidentiality Label Syntax” and “Binding of Metadata to Data Objects” specifications.

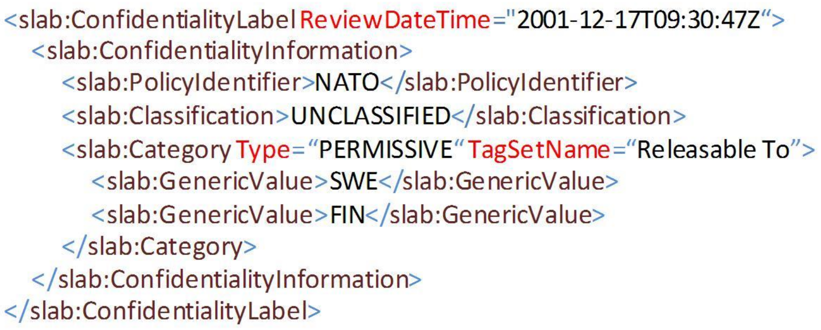
[6] Note that this is a mock example. The correspondence between original and alternative confidentiality label must be agreed upon bilaterallly between nations and NATO.

5.2 NATO Profile for the XML Confidentiality Label Syntax

The NATO profile is a recommendation for standardized usage of the XML Confidentiality Label syntax within NATO. It is inherited from the XML Confidentiality Label syntax and further specifies the usage of attributes, categories and their values. The values that can be contained by the several XML elements are not defined in the profile but must be in accordance with NATO policy.

The NATO profile for XML Confidentiality Labels contains a recommended syntax for both eye readable and machine readable labels. Eye readable (confidentiality) labels are typically used in environments in which ACDF do not support machine readable labels, and/or in which there is no access to a NATO Security Policy Information File (SPIF)[7]. Alternatively, eye readable labels might be useful when a label is only processed in order to display its contents, or when it is expected to be interpreted by humans only.

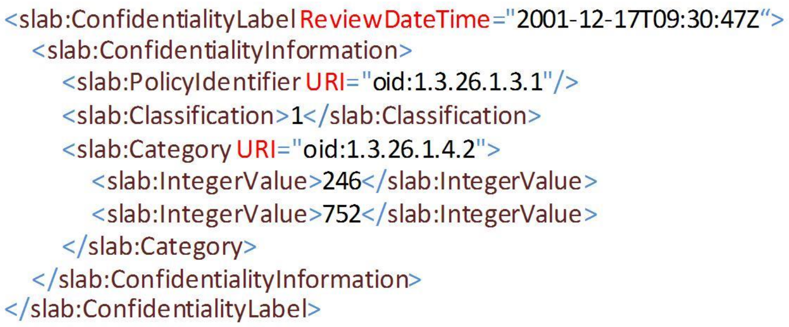
Below are two examples showing a eye readable (Figure 4) and a machine readable (Figure 5) confidentiality label with release categories, created under NATO policy.



```
<slab:ConfidentialityLabel ReviewDateTime="2001-12-17T09:30:47Z“>
  <slab:ConfidentialityInformation>
    <slab:PolicyIdentifier>NATO</slab:PolicyIdentifier>
    <slab:Classification>UNCLASSIFIED</slab:Classification>
    <slab:Category Type=“PERMISSIVE“ TagSetName=“Releasable To”>
      <slab:GenericValue>SWE</slab:GenericValue>
      <slab:GenericValue>FIN</slab:GenericValue>
    </slab:Category>
  </slab:ConfidentialityInformation>
</slab:ConfidentialityLabel>
```

Figure 4: Example of an eye readable XML based confidentiality label. The GenericValue element allows for any text string; however the attribute TagSetName was defined so that ACDF can act solely on the relevant Access Control Information (e.g. 'FIN', or 'SWE')

Figure 5 below shows the machine readable equivalent of the example in Figure 4. The specification defines a URI attribute which can contain a reference to applicable policy or predefined value sets (e.g. for classification or categories). Within NATO such a reference is commonly provided by an object identifier (oid). The example in Figure 5 shows the use of common NATO oids.



```
<slab:ConfidentialityLabel ReviewDateTime="2001-12-17T09:30:47Z“>
  <slab:ConfidentialityInformation>
    <slab:PolicyIdentifier URI="oid:1.3.26.1.3.1"/>
    <slab:Classification>1</slab:Classification>
    <slab:Category URI="oid:1.3.26.1.4.2">
      <slab:IntegerValue>246</slab:IntegerValue>
      <slab:IntegerValue>752</slab:IntegerValue>
    </slab:Category>
  </slab:ConfidentialityInformation>
</slab:ConfidentialityLabel>
```

Figure 5: Machine readable equivalent of the example in Figure 4. Oid values are used to reference the unique NATO policy and category sets that are applicable. This way the values of the classification element and the category child elements can be interpreted uniquely

[7] Machine readable ACDF typically make use of a Security Policy Identification File (SPIF) to verify the values used in a (sensitivity) label. Such a SPIF exists for NATO but has not been formally standardized yet.

5.3 NATO Profile for the Binding of Metadata to Data Objects

The NATO profile is a recommendation for standardized usage of the “Binding of Metadata to Data Objects” specification. The profile proposes the semantics for the binding of metadata to XML using XMLDSIG and prescribes a use of XMLDSIG that takes the security considerations and requirements for conformance to NATO policy into account. The profile is based on the original version of XMLDSIG, however it recommends some features that only exist in the 2nd edition [3]. The NATO profile lists the requirements for the use of transform algorithms, canonicalization methods, digest methods and signature methods.

6.0 NATO CWID 2009 DEMONSTRATION

Having developed specifications for both binding and labelling, cross-domain sharing experiments were set up within the context of the NATO Coalition Warrior Interoperability Demonstration (CWID) 2009. The use of XML based labels and the XMLDSIG based strong binding mechanism was successfully demonstrated and involved trials between NC3A and a number of NATO nations including Norway, UK, France and Germany. The trials focussed on the integration of XML-Labelling in Command and Control (C2) applications[8] as well as granular access control offered by XML guards[9].

Figure 6 below shows an example of a trial that focussed on the application of XML -labelling to the data objects and information exchange scenarios in the geo services community. In this trial a client in a simulated low network enclave accesses image files or map data on a server in a simulated high network enclave. The image files and map data are labelled following the proposed specifications, and the NC3A XML-Labelling Guard mediated the data flow while enforcing a release policy. Due to the map layer information being formatted in XML, it was possible to apply granular labelling in the sense that different confidentiality labels could be bound to different map layers. The NC3A XML-Labelling Guard was then able to remove map layers that were not releasable to the low enclave.

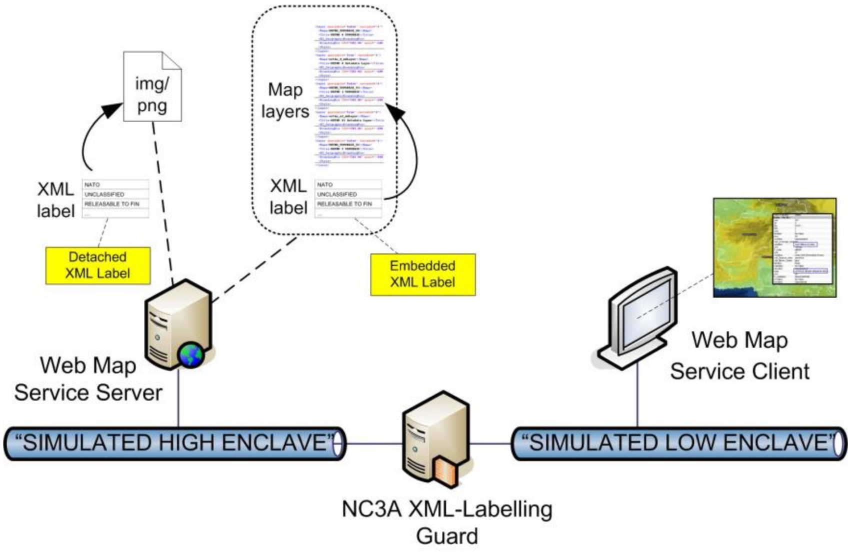


Figure 6: Setup of one of the CWID 2009 trials; a server responds with XML-labelled geo services data. Either an XML label is embedded in an XML document – labelling map layers separately with different classification and release levels – or it is detached and bound to image files

[8] These included Friendly Force Tracking, GeoServices and Web Browsing.

[9] XML guards were provided by UK, Norway (FFI) and NC3A (XML-Labelling Guard).

Further details on the CWID trials can be provided by the authors upon request.

7.0 CONCLUSIONS AND FUTURE WORK

This paper provided an overview of the specifications "XML Confidentiality Label Syntax" and "Binding of Metadata to Data Objects" that have been developed by NATO Research Task Group on XML in Cross Domain Security Solutions (IST-068/RTG-031). The proposed specifications aim to realize a standardized approach to binding any type of metadata (such as the traditional security marking) to any type of data objects, while supporting the concept of OLP in NNEC. Experimentation at CWID 2009 have shown that cross-domain sharing can be enabled with access control at a fine level of granularity so that automated redaction of information, performed by guards at the cross domain boundary, becomes possible.

To further the adaptation of the proposed specification within NATO, NC3A is developing NATO profiles that aim to standardize the use of the specifications within NATO. In addition, objectives for 2010 will be to realize inclusion of schemas and name spaces associated to both proposed specifications in the NATO Metadata Registry and Repository as well as to develop standard profiles for inclusion in the NATO Interoperability Standards and Profiles Repository. The next step will be to initiate formal procedures towards acceptance as a NATO standard.

Although the NATO profiles are meant to standardize the use of the proposed specifications, there is still a lot of liberty in applying the specifications to data objects and protocols. Therefore, application profiles should be written that provide guidance on how to integrate XML Confidentiality Labels and the associated binding in common office applications (e.g. Microsoft Office, OpenOffice) and with application protocols such as the Simple Object Access Protocol (SOAP). Such application profiles will also be influenced by the information exchange scenario that is supported. At the Coalition Warrior Interoperability Exercise (CWIX) 2010 a number of nations will further experiment with the proposed specifications. Future experimentation should also focus on the integration of the use of XML-labelling with other common client-side applications.

The proposed specifications described in this paper define how any type of metadata can be bound to any type of data object. However, the derivation of requirements for confidentiality protection as well as the actual implementation of this protection for a given data object and metadata binding will be the topic of future research in the area of OLP. Future research should also cover the integration of OLP in document management system architectures.

REFERENCES

[1] NATO Research and Technology Organization document RTO RTG-031/IST-068 "XML In Cross-Domain Security Solutions", RTO, Paris, FR, 2010.

[2] XML Signature Working Group (on-line), http://www.w3.org/, 'XML-Signature Syntax and Processing', at http://www.w3.org/TR/xmldsig-core/, W3C Recommendation, World Wide Web Consortium, Cambridge, US, 12 February 2002.

[3] XML Signature Working Group (on-line), http://www.w3.org/, 'XML- Signature Syntax and Processing (Second Edition)', at http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/, W3C Recommendation, World Wide Web Consortium, Cambridge, US, 10 June 2008.